WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Tuesday, March 09, 2004

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=ADJ	
☐	L23	L21 and 709/2$$.ccls.	11
☐	L22	L21 and l7	3
☐	L21	detect$ same interrupt$ same terminal same network	274
☐	L20	detect$ same interrupt$ same terminal	4834
☐	L19	l18 and condition	8
☐	L18	L17 and l7	9
☐	L17	709/2$$.ccls. and L16	9
☐	L16	L15 and l7	27
☐	L15	l5 same interrupt$	193
☐	L14	L13 and 709/2$$.ccls.	5
☐	L13	l11 and L12	26
☐	L12	client and server	20460
☐	L11	diagnos$ and L10	81
☐	L10	l6 and l7	137
☐	L9	l7 and L8	1
☐	L8	judg$4 same l3	10893
☐	L7	(reestablish$4 or re-establish$4) and L6	137
☐	L6	L5 and l4	681
☐	L5	L1 same l2	3108
☐	L4	communication same l3	46079
☐	L3	interrupt$ or stop$	961306
☐	L2	(detect$ or discover$) same (network) same failure$	3108
☐	L1	network or internet	289777

END OF SEARCH HISTORY

h e b b cg b chh e g f c e h

WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Tuesday, March 09, 2004

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=ADJ	
☐	L18	L17 and l7	9
☐	L17	709/2$$.ccls. and L16	9
☐	L16	L15 and l7	27
☐	L15	l5 same interrupt$	193
☐	L14	L13 and 709/2$$.ccls.	5
☐	L13	l11 and L12	26
☐	L12	client and server	20460
☐	L11	diagnos$ and L10	81
☐	L10	l6 and l7	137
☐	L9	l7 and L8	1
☐	L8	judg$4 same l3	10893
☐	L7	(reestablish$4 or re-establish$4) and L6	137
☐	L6	L5 and l4	681
☐	L5	L1 same l2	3108
☐	L4	communication same l3	46079
☐	L3	interrupt$ or stop$	961306
☐	L2	(detect$ or discover$) same (network) same failure$	3108
☐	L1	network or internet	289777

END OF SEARCH HISTORY

h e b b cg b chh e g f ff e ch e h

L18: Entry 2 of 9 File: USPT Sep 18, 2001

DOCUMENT-IDENTIFIER: US 6292905 B1
**** See image for Certificate of Correction ****
TITLE: Method for providing a fault tolerant network using distributed server processes to remap clustered network resources to other servers during server failure

Abstract Text (1):
The method of the current invention provides a fault tolerant access to a network resource. A replicated network directory database operates in conjunction with server resident processes to remap a network resource in the event of a server failure. The records/objects in the replicated database contain for each network resource, a primary and a secondary server affiliation. Initially, all users access a network resource through the server identified in the replicated database as being the primary server for the network resource. When server resident processes detect a failure of the primary server, the replicated database is updated to reflect the failure of the primary server, and to change the affiliation of the network resource from its primary to its backup server. This remapping occurs transparently to whichever user/client is accessing the network resource. As a result of the remapping, all users access the network resource through the server identified in the replicated database as the backup server for the resource. When the server resident processes detect a return to service of the primary server, the replicated database is again updated to reflect the resumed operation of the primary server. This remapping of network resource affiliations also occurs transparently to whichever user/client is accessing the network resource, and returns the resource to its original fault tolerant state.

Brief Summary Text (12):
To prevent network down-time due to a print/file server, server mirroring has been developed. Server mirroring as it is currently implemented requires a primary server and storage device, a backup server and storage device, and a unified operating system linking the two. An example of a mirrored server product is the Software Fault Tolerance level 3 (SFT III) product by Novell Inc., 1555 North Technology Way, Orem, Utah, as an add-on to its NetWare.RTM. 4.x product. SFT III maintains servers in an identical state of data update. It separates hardware-related operating system (OS) functions on the mirrored servers so that a fault on one hardware platform does not affect the other. The server OS is designed to work in tandem with two servers. One server is designated as a primary server, and the other is a secondary server. The primary server is the main point of update; the secondary server is in a constant state of readiness to take over. Both servers receive all updates through a special link called a mirrored server link (MSL), which is dedicated to this purpose. The servers also communicate over the local area network (LAN) that they share in common, so that one knows if the other has failed even if the MSL has failed. When a failure occurs, the second server automatically takes over without interrupting communications in any user-detectable way. Each server monitors other server's NetWare Core Protocol (NCP) acknowledgments over the LAN to see that all the requests are serviced and that OSs are constantly maintained in a mirrored state.

Detailed Description Text (2):
The method of the current invention provides a fault tolerant network without

hardware mirroring. The invention involves an enhanced replicated network directory database which operates in conjunction with server resident processes to remap network resources in the event of a server failure. In some embodiments, the enhanced network directory database is replicated throughout all servers in the cluster. The records/objects in the enhanced database contain for at least 1 clustered resource, a primary and a secondary server affiliation. Initially, all users access a clustered resource through the server identified in the enhanced database as being the primary server for that clustered resource. When server resident processes detect a failure of the primary server the enhanced database is updated to reflect the failure of the primary server, and to change the affiliation of the resource from its primary to its backup server. The updating and remapping is accomplished by server resident processes which detect failure of the primary server, and remap the network resource server affiliation. This remapping occurs transparently to whichever user/client is accessing the resource. Thus, network communications are not interrupted and all users access a resource through its backup server, while its primary server is out of operation. This process may be reversed when the primary server resumes operation, thereby regaining fault tolerant, i.e., backup capability.

Detailed Description Text (14):
FIG. 3 is a hardware block diagram of an embodiment of the current invention in a local area network. Users A-D are shown interfacing via workstations 66-72 with network resources. The network resources include servers 54-58, storage devices 78-82 and printers 84-86, for example. The relationship between network resources is defined not only as discussed above in connection with FIGS. 1-2 for normal operation, but also for operation in the event of a failure of any one of the network resources. This additional utility, i.e., fault tolerance is a result of enhancements to the network directory databases 150A-C and processes 152A-C resident on each server. The server resident processes operating in conjunction with the enhanced network directory database allow failure detection, resource/object remapping and recovery. Thus, network downtime is reduced by transparently remapping network resources in response to a detection of a failure. The remapped route is defined within the enhanced directory. The routes that are defined in the directory may be part of the initial administrative setup; or may be a result of an automatic detection process; or may be a result of real time arbitration between servers. The server resident processes 152A-C have the additional capability of returning the resource/network to its initial configuration when the failed resource has been returned to operation. This latter capability is also a result of the interaction between the host resident processes 152A-C and the enhanced network directory 150A-C.

Detailed Description Text (18):
As shown in FIG. 5C, process 152B running on server 54 has detected the failure of server 56 and has remapped communications between workstation 68 and storage device 80 via server 54. This remapping is the result of the process 152B running on server 54. These processes have detected the failure of server 56. They have determined on the basis of backup property values for storage device 80 stored in the enhanced network directory database 150B that server 54 can provide backup capability for storage device 80. Finally, they have altered the property values on the object/record for storage device 80 within the enhanced network directory database to cause communications with the storage device 80 to be re-routed through server 54.

Detailed Description Text (20):
In FIG. 5E updated replicas 150A-B of the network directory database are present on respectively servers 56-54. Processes 152A-B running on respectively servers 56-54 have caused the network to be reconfigured to its original architecture in which server 56 is the means by which workstation 68, for example, communicates with storage device 80. This fail-back is a result of several acts performed cooperatively by processes 152A-B. Process 152B detects re-enablement of server 56.

Process 152B relinquishes ownership of storage device 80 by server 54. Process 152A running on server 56, detects relinquishment of ownership of storage device 80 by server 54 and in response thereto updates the host server property value for resource/object storage device 80 in the replicated network directory database. Communications between workstation 68 and storage device 80 are re-established via server 56, as indicated by communication marker 252. All of these processes may take place transparently to the user, so as not to interrupt network service. During the period of fail-over, server 54 handles communications to both storage device 78 as well as storage device 80.

Detailed Description Text (22):
FIG. 6A shows an initial condition in which the host server property variable 110A/B and the primary server property value 210A/B match. In FIG. 6B, server 54 has failed and therefore the replica of the enhanced network directory database and each of the objects within that directory are no longer available as indicated by failure mark 258. Nevertheless, an up-to-date current replica of the enhanced network directory database is still available on server 56 as indicated by objects 200B and 202B on the right-hand side of FIG. 6B. In FIG. 6C, the fail-over corresponding to that discussed above in connection with FIG. 5C is shown. The host server property value 110B has been updated to reflect current network routing during the failure of server 56. The host server property value 110B is server 54. Because the resource/object for storage device 80 appears on all servers as server 54, all communications between workstations, i.e., workstation 68 are re-routed through server 54 to storage device 80. The fail-over is accomplished by resident process 152B on server 54 [see FIGS. 5A-E]. These processes detect the failure of server 56. Then they determine which server is listed in the resource/object record for storage device 80 as a backup. Next the processes write the backup property value to the host property value for storage device 80. Replicas of this updated set of property value(s) for object 200B, corresponding to the storage device 80, are then replicated throughout the network. As indicated in FIG. 6C, the prior state property value 220B is updated by the resident process 152B [see FIGS. 5A-E] to indicate that a fail-over has taken place.

Detailed Description Text (26):
Modules 322-328 may interact with the above discussed modules to provide the server resident processes for detection, fail-over and fail-back. Module 322 may handle communications with a user through network user terminal module 306. Module 322 may also be responsible for sending and receiving packets through NCP module 308 to manage failure detection and recovery detection of a primary server. Module 324, the directory services manager, may be responsible for communicating through module 320 with the enhanced network directory database 150A. Module 324 controls the addition of properties as well as the viewing, and editing of property values within that database. Module 326 is a device driver which in a current embodiment superimposes a phase shifted signal on the peripheral communications between a server and its direct connected resources to detect server failure. Module 326 sends and receives these phase shifted signals through module 316. Module 328 controls the overall interaction of modules 322-326. In addition, module 328 interfaces with module 312 to scan, mount and dismount objects/resources. Furthermore, module 328 interacts with module 314 to obtain device hardware identifiers for those devices which are direct attached to the server. The interaction of each of these modules to provide for detection, fail-over and fail-back will be discussed in detail in the following FIGS. 8A-C.

Detailed Description Text (33):
The processes run on the backup server in connection with failure-detection and fail-over are initiated at splice block B, which is shown on the right-hand side of FIG. 8B. Control passes from splice block B to processes 402-404. In process 402 the backup server continually monitors the LAN communication between itself and the primary server to determine when the primary server has failed. It does this by determining the primary server ID from the host server property value 110A [FIG.

4]. This object property ID is appended by the LAN detector module 322 to network control protocol packets. These packets are sent intermittently by the network control protocol module 308 [see FIG. 7] on the backup server to the primary server to determine when the primary server fails. Control is then passed to decision process 406. In decision process 406 the backup server monitors across connection 250 [see FIGS. 5A-E] the drive pulse discussed above in connection with process 400. These pulses can be used to determine when the connection from the primary server to the storage device has failed. Control then passes to decision process 406.

Detailed Description Text (34):
In decision process 406, a determination is made as to whether on the basis of LAN communications, the primary server has failed. In the event this determination is in the negative, control returns to processes 402 and 404. Alternately, if this determination is in the affirmative i.e., that the primary server is no longer responding to the secondary server's NCP packets, then control is passed to decision process 408. In decision process 408, a determination is made as to whether the drive pulse from the primary is still being received by the secondary server across connection 250. If a determination is made that the communication between the primary server and the storage device 80 has not failed, i.e., that the drive monitor is still detecting drive pulses from the primary, then control returns to processes 402 and 404. This secondary drive detection assures that a momentary LAN failure will not result in the determination that the primary server has failed when in fact that primary server still is communicating with the resource/object such as storage device 80 [See FIGS. 5A-E]. In the alternative, if determination is reached in decision process 408 that the primary server is no longer communicating with the resource/object, then control is passed to the process 410. In process 410 the user is notified of the failure of a primary server. The notification occurs through the cooperative operation of modules 328, 322 and 308 discussed above in connection with FIG. 7. Control is then passed to process 412. In process 412 the secondary server activates the object and passes control to process 414. In process 414 the secondary server mounts the object i.e., physically assumes control over the object. Control is then passed to process 416 in which the secondary server writes into the host server property value 110A the value for its ID in place of the primary server ID. This new property value is then replicated across all enhanced network directory databases on all the servers in the enterprise. Thus, a failure has been detected and transparently to the user an alternate path for communications between workstations and the object, e.g. storage device 80, through the secondary server, e.g. server 54. [See FIGS. 5A-E]. Control then passes to process 418 in which the object is reserved by the backup server.

Detailed Description Paragraph Table (1):
Application Attorney Docket Title No. No. "System Architecture for Remote 08/942,160 MNFRAME.002A1 Access and Control of Environmental Management" "Method of Remote Access and 08/942,215 MNFRAME.002A2 Control of Environmental Management" "System for Independent Powering of 08/942,410 MNFRAME.002A3 Diagnostic Processes on a Computer System" "Method of Independent Powering of 08/942,320 MNFRAME.002A4 Diagnostic Processes on a Computer System" "Diagnostic and Managing 08/942,402 MNFRAME.005A1 Distributed Processor System" "Method for Managing a 08/942,448 MNFRAME.005A2 Distributed Processor System" "System for Mapping Environmental 08/942,222 MNFRAME.005A3 Resources to Memory for Program Access" "Method for Mapping Environmental 08/942,214 MNFRAME.005A4 Resources to Memory for Program Access" "Hot Add of Devices Software 08/942,309 MNFRAME.006A1 Architecture" "Method for The Hot Add of 08/942,306 MNFRAME.006A2 Devices" "Hot Swap of Devices Software 08/942,311 MNFRAME.006A3 Architecture" "Method for The Hot Swap of 08/942,457 MNFRAME.006A4 Devices" "Method for the Hot Add of a 08/943,072 MNFRAME.006A5 Network Adapter on a System Including a Dynamically Loaded Adapter Driver" "Method for the Hot Add of a 08/942,069 MNFRAME.006A6 Mass Storage Adapter on a System Including a Statically Loaded Adapter Driver" "Method for the Hot Add of a 08/942,465 MNFRAME.006A7 Network Adapter on a System Including a Statically Loaded

Adapter Driver" "Method for the Hot Add of a 08/962,963 MNFRAME.006A8 Mass Storage Adapter on a System Including a Dynamically Loaded Adapter Driver" "Method for the Hot Swap of a 08/943,078 MNFRAME.006A9 Network Adapter on a System Including a Dynamically Loaded Adapter Driver" "Method for the Hot Swap of a 08/942,336 MNFRAME.006A- Mass Storage Adapter on a System 10 Including a Statically Loaded Adapter Driver" "Method for the Hot Swap of a 08/942,459 MNFRAME.006A- Network Adapter on a System 11 Including a Statically Loaded Adapter Driver" "Method for the Hot Swap of a 08/942,458 MNFRAME.006A- Mass Storage Adapter on a System 12 Including a Dynamically Loaded Adapter Driver" "Method of Performing an Extensive 08/942/463 MNFRAME.008A Diagnostic Test in Conjunction with a BIOS Test Routine" "Apparatus for Performing an 08/942,463 MNFRAME.009A Extensive Diagnostic Test in Conjunction with a BIOS Test Routine" "Configuration Management Method 08/941,268 MNFRAME.010A for Hot Adding and Hot Replacing Devices" "Configuration Management System 08/942,408 MNFRAME.011A for Hot Adding and Hot Replacing Devices" "Apparatus for Interfacing Buses" 08/942,382 MNFRAME.012A "Method for Interfacing Buses" 08/942,413 MNFRAME.013A "Computer Fan Speed Control 08/942,447 MNFRAME.016A Device" "Computer Fan Speed Control 08/942,216 MNFRAME.017A Method" "System for Powering Up and 08/943,076 MNFRAME.018A Powering Down a Server" "Method for Powering Up and 08/943,077 MNFRAME.019A Powering Down a Server" "System for Resetting a Server" 08/942,333 MNFRAME.020A "Method for Resetting a Server" 08/942,405 MNFRAME.021A "System for Displaying Flight 08/942,070 MNFRAME.022A Recorder" "Method for Displaying Flight 08/942,068 MNFRAME.023A Recorder" "Synchronous Communication 08/943,355 MNFRAME.024A Interface" "Synchronous Communication 08/942,004 MNFRAME.025A Emulation" "Software System Facilitating 08/942,317 MNFRAME.026A the Replacement or Insertion of Devices in a Computer System" "Method for Facilitating the 08/942,316 MNFRAME.027A Replacement or Insertion of Devices in a Computer System" "System Management Graphical 08/943,357 MNFRAME.028A User Interface" "Display of System Information" 08/942,195 MNFRAME.029A "Data Management System 08/942,129 MNFRAME.030A Supporting Hot Plug Operations on a Computer" "Data Management Method 08/942,124 MNFRAME.031A Supporting Hot Plug Operations on a Computer" "Alert Configurator and Manager" 08/942,005 MNFRAME.032A "Managing Computer System Alerts" 08/943,356 MNFRAME.033A "Computer Fan Speed Control 08/940,301 MNFRAME.034A System" "Computer Fan Speed Control 08/941,267 MNFRAME.035A System Method" "Black Box Recorder for 08/942,381 MNFRAME.036A Information System Events" "Method of Recording Information 08/942,164 MNFRAME.037A System Events" "Method for Automatically 08/942,168 MNFRAME.040A Reporting a System Failure in a Server" "System for Automatically 08/942,384 MNFRAME.041A Reporting a System Failure in a Server" "Expansion of PCI Bus Loading 08/942,404 MNFRAME.042A Capacity" "Method for Expanding of PCI 08/942,223 MNFRAME.043A Bus Loading Capacity" "System for Displaying System 08/942,347 MNFRAME.044A Status" "Method of Displaying System 08/942,071 MNFRAME.045A Status" "Fault Tolerant Computer 08/942,194 MNFRAME.046A System" "Method for Hot Swapping of 08/943,044 MNFRAME.047A Network Components" "A Method for Communicating a 08/942,221 MNFRAME.048A Software Generated Pulse Waveform Between Two Servers in a Network" "A System for Communicating a 08/942,409 MNFRAME.049A Software Generated Pulse Waveform Between Two Servers in a Network" "Method for Clustering Software 08/942,318 MNFRAME.050A Applications" "System for Clustering Software 08/942,411 MNFRAME.051A Applications" "Method for Automatically 08/942,319 MNFRAME.052A Configuring a Server after Hot Add of a Device" "System for Automatically 08/942,331 MNFRAME.053A Configuring a Server after Hot Add of a Device" "Method of Automatically 08/942,412 MNFRAME.054A Configuring and Formatting a Computer System and Installing Software" "System for Automatically 08/941,955 MNFRAME.055A Configuring and Formatting a Computer System and Installing Software" "Determining Slot Numbers in 08/942,462 MNFRAME.056A a Computer" "System for Detecting Errors 08/942,169 MNFRAME.058A in a Network" "Method of Detecting Errors 08/940,302 MNFRAME.059A in a Network" "System for Detecting Network 08/942,407 MNFRAME.060A Errors" "Method of Detecting Network 08/942,573 MNFRAME.061A Errors"

Current US Cross Reference Classification (1):
709/239

h e b b g e e e f c e g e ge

CLAIMS:

1. A method for fault tolerant access to a network resource, on a network with a client workstation and a first and a second server, said method for fault tolerant access comprising the acts of:

selecting a first server to provide communications between a client workstation and a network resource;

detecting a failure of the first server, comprising the acts of:

monitoring across a common bus, at a second server, communications between the first server and the network resource across the common bus by noting a continual change in state of the network resource, and

observing a termination in the communications between the first server and the network resource across the common bus by noting a stop in the continual change in state of the network resource; and

routing communications between the client workstation and the network resource via the second server.

7. The method for fault tolerant access to a network resource of claim 5, wherein said act of detecting a failure of the first server, further includes the acts of:

reading the second field in the first record of the network resource database;

determining on the basis of said reading act that the second field identifies the backup server for the network resource as the second server;

activating the monitoring by the second server of the first server, in response to said determining act; and

ascertaining at the second server a failure of the first server.

10. A program storage device encoding instructions for:

causing a computer to provide a network resource database, the database including individual records corresponding to network resources, and the network resource database including a first record corresponding to the network resource and the first record identifying a primary server for the network resource as a first server;

causing a computer to select, on the basis of the first record, the first server to provide communications between a client workstation and the network resource;

causing a computer to recognize the backup server for the network resource as the second server;

causing a computer to detect a failure of the first server, including:

causing a computer to monitor across a common bus, at the second server, communications between the first server and the network resource across the common bus by noting a continual change in state of the network resource, and

causing a computer to observe a termination in the communications between the first server and the network resource across the common bus by noting a stop in the continual change in state of the network resource; and

causing a computer to route communications between the client workstation and the network resource via the second server, responsive to said recognizing and detecting acts.

19. A method for providing fault tolerant access to a network resource, on a network with a client workstation and a first and a second server and a network resource database, wherein the network resource database includes a first record corresponding to a network resource and the first record includes a first field containing the name of the network resource and a second field containing the host server affiliation of the network resource; said method for fault tolerant access comprising the acts of:

expanding the network resource database to include a third field for naming the primary server affiliation for the network resource and a fourth field for naming the backup server affiliation for the network resource;

naming the first server in the third field;

selecting, on the basis of the first record, the first server to provide communications between the client workstation and the network resource;

naming the second server in the fourth field;

recognizing, on the basis of the fourth field of the first record, the backup server for the network resource as the second server;

detecting a failure of the first server, including the acts of:

monitoring across a common bus, at the second server, communications between the first server and the network resource across the common bus by noting a continual change in state of the network resource, and

observing a termination in the communications between the first server and the network resource across the common bus by noting a stop in the continual change in state of the network resource; and

routing communications between the client workstation and the network resource via the second server, responsive to said recognizing and detecting acts.

23. The method for fault tolerant access to a network resource of claim 19, wherein said act of detecting a failure of the first server, further includes the acts of sending

sending packets intermittently from the second server to the first server;

receiving acknowledgments from the first server at the second server, the acknowledgments responsive to said sending act; and

noticing a termination in the receipt of acknowledgments from the first server.

24. A computer usable medium having computer readable program code means embodied therein for causing fault tolerant access to a network resource on a network with a client workstation and a first and second server, and a network resource database, wherein the network resource database includes a first record corresponding to a network resource and the first record includes a first field containing the name of the network resource and a second field containing the host server affiliation of the network resource; the computer readable program code means in said article of manufacture comprising;

computer readable program code means for causing a computer to expand the network

resource database to include a third field for naming the primary server affiliation for the network resource and a fourth field for naming the backup server affiliation for the network resource;

computer readable program code means for causing a computer to name the first server in the third field;

computer readable program code means for causing a computer to select, on the basis of the first record, the first server to provide communications between the client workstation and the network resource;

computer readable program code means for causing a computer to name the second server in the fourth field;

computer readable program code means for causing a computer to recognize, on the basis of the fourth field of the first record, the backup server for the network resource as the second server;

computer readable program code means for monitoring across a common bus, at a second server, communications between the first server and the network resource across the common bus by noting a continual change in state of the network resource, and observing a termination in the communications between the first server and the network resource across the common bus by noting a stop in the continual change in state of the network resource; and

computer readable program code means for causing a computer to route communications between the client workstation and the network resource via the second server, responsive to said recognizing and detecting acts.

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 26 of 26 returned.

☐ 1. Document ID: US 6636721 B2

L13: Entry 1 of 26 File: USPT Oct 21, 2003

US-PAT-NO: 6636721
DOCUMENT-IDENTIFIER: US 6636721 B2

TITLE: Network engineering/systems system for mobile satellite communication system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWMC | Draw. De

☐ 2. Document ID: US 6633835 B1

L13: Entry 2 of 26 File: USPT Oct 14, 2003

US-PAT-NO: 6633835
DOCUMENT-IDENTIFIER: US 6633835 B1

TITLE: Prioritized data capture, classification and filtering in a network monitoring environment

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWMC | Draw. De

☐ 3. Document ID: US 6625750 B1

L13: Entry 3 of 26 File: USPT Sep 23, 2003

US-PAT-NO: 6625750
DOCUMENT-IDENTIFIER: US 6625750 B1

TITLE: Hardware and software failover services for a file server

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWMC | Draw. De

☐ 4. Document ID: US 6542739 B1

L13: Entry 4 of 26 File: USPT Apr 1, 2003

US-PAT-NO: 6542739

h e b b g e e e f e g ef b e

DOCUMENT-IDENTIFIER: US 6542739 B1

TITLE: Priority and preemption service system for satellite related communication using central controller

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWMC | Draw De

---

☐ 5. Document ID: US 6529731 B2

L13: Entry 5 of 26 File: USPT Mar 4, 2003

US-PAT-NO: 6529731
DOCUMENT-IDENTIFIER: US 6529731 B2

TITLE: Network control center for satellite communication system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWMC | Draw De

---

☐ 6. Document ID: US 6494831 B1

L13: Entry 6 of 26 File: USPT Dec 17, 2002

US-PAT-NO: 6494831
DOCUMENT-IDENTIFIER: US 6494831 B1

TITLE: Medical diagnostic system service connectivity method and apparatus

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWMC | Draw De

---

☐ 7. Document ID: US 6421711 B1

L13: Entry 7 of 26 File: USPT Jul 16, 2002

US-PAT-NO: 6421711
DOCUMENT-IDENTIFIER: US 6421711 B1

TITLE: Virtual ports for data transferring of a data storage system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWMC | Draw De

---

☐ 8. Document ID: US 6411806 B1

L13: Entry 8 of 26 File: USPT Jun 25, 2002

US-PAT-NO: 6411806
DOCUMENT-IDENTIFIER: US 6411806 B1

TITLE: Virtual network configuration and management system for satellite communications system

h e b b g e e e f e g ef b e

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 9. Document ID: US 6292905 B1

L13: Entry 9 of 26 File: USPT Sep 18, 2001

US-PAT-NO: 6292905
DOCUMENT-IDENTIFIER: US 6292905 B1
**** See image for Certificate of Correction ****

TITLE: Method for providing a fault tolerant network using distributed server processes to remap clustered network resources to other servers during server failure

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 10. Document ID: US 6272341 B1

L13: Entry 10 of 26 File: USPT Aug 7, 2001

US-PAT-NO: 6272341
DOCUMENT-IDENTIFIER: US 6272341 B1

TITLE: Network engineering/systems engineering system for mobile satellite communication system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 11. Document ID: US 6272338 B1

L13: Entry 11 of 26 File: USPT Aug 7, 2001

US-PAT-NO: 6272338
DOCUMENT-IDENTIFIER: US 6272338 B1

TITLE: Network control center for satellite communication system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 12. Document ID: US 6260120 B1

L13: Entry 12 of 26 File: USPT Jul 10, 2001

US-PAT-NO: 6260120
DOCUMENT-IDENTIFIER: US 6260120 B1

TITLE: Storage mapping and partitioning among multiple host processors in the presence of login state changes and host controller replacement

h e b b g e e e f e g ef b e

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 13. Document ID: US 6243580 B1

L13: Entry 13 of 26 File: USPT Jun 5, 2001

US-PAT-NO: 6243580
DOCUMENT-IDENTIFIER: US 6243580 B1
**** See image for Certificate of Correction ****

TITLE: Priority and preemption service system for satellite related communication using central controller

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 14. Document ID: US 6243361 B1

L13: Entry 14 of 26 File: USPT Jun 5, 2001

US-PAT-NO: 6243361
DOCUMENT-IDENTIFIER: US 6243361 B1
**** See image for Certificate of Correction ****

TITLE: Multistage interconnect network uses a master processor to perform dynamic configuration for all switch nodes based on a predetermined topology

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 15. Document ID: US 6185409 B1

L13: Entry 15 of 26 File: USPT Feb 6, 2001

US-PAT-NO: 6185409
DOCUMENT-IDENTIFIER: US 6185409 B1

TITLE: Network engineering/systems engineering system for mobile satellite communication system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 16. Document ID: US 6112085 A

L13: Entry 16 of 26 File: USPT Aug 29, 2000

US-PAT-NO: 6112085
DOCUMENT-IDENTIFIER: US 6112085 A

TITLE: Virtual network configuration and management system for satellite communication system

h e b b g e e e f e g ef b e

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 17. Document ID: US 6058307 A

L13: Entry 17 of 26 File: USPT May 2, 2000

US-PAT-NO: 6058307
DOCUMENT-IDENTIFIER: US 6058307 A

TITLE: Priority and preemption service system for satellite related communication using central controller

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 18. Document ID: US 5987621 A

L13: Entry 18 of 26 File: USPT Nov 16, 1999

US-PAT-NO: 5987621
DOCUMENT-IDENTIFIER: US 5987621 A

TITLE: Hardware and software failover services for a file server

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 19. Document ID: US 5913164 A

L13: Entry 19 of 26 File: USPT Jun 15, 1999

US-PAT-NO: 5913164
DOCUMENT-IDENTIFIER: US 5913164 A

TITLE: Conversion system used in billing system for mobile satellite system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 20. Document ID: US 5881131 A

L13: Entry 20 of 26 File: USPT Mar 9, 1999

US-PAT-NO: 5881131
DOCUMENT-IDENTIFIER: US 5881131 A

TITLE: Analysis and validation system for provisioning network related facilities

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

h e b b g e e e f e g ef b e

☐ 21. Document ID: US 5872904 A

L13: Entry 21 of 26 File: USPT Feb 16, 1999

US-PAT-NO: 5872904
DOCUMENT-IDENTIFIER: US 5872904 A

TITLE: Computer system using a master processor to automatically reconfigure faulty switch node that is detected and reported by diagnostic processor without causing communications interruption

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

☐ 22. Document ID: US 5842125 A

L13: Entry 22 of 26 File: USPT Nov 24, 1998

US-PAT-NO: 5842125
DOCUMENT-IDENTIFIER: US 5842125 A

TITLE: Network control center for satellite communication system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

☐ 23. Document ID: US 5713075 A

L13: Entry 23 of 26 File: USPT Jan 27, 1998

US-PAT-NO: 5713075
DOCUMENT-IDENTIFIER: US 5713075 A

TITLE: Network engineering/systems engineering system for mobile satellite communication system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

☐ 24. Document ID: US 5522046 A

L13: Entry 24 of 26 File: USPT May 28, 1996

US-PAT-NO: 5522046
DOCUMENT-IDENTIFIER: US 5522046 A
**** See image for Certificate of Correction ****

TITLE: Communication system uses diagnostic processors and master processor module to identify faults and generate mapping tables to reconfigure communication paths in a multistage interconnect network

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

h e b b g e e e f e g ef b e

☐ 25. Document ID: US 5321813 A

L13: Entry 25 of 26 File: USPT Jun 14, 1994

US-PAT-NO: 5321813
DOCUMENT-IDENTIFIER: US 5321813 A

TITLE: Reconfigurable, fault tolerant, multistage interconnect network and protocol

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

☐ 26. Document ID: US 5303383 A

L13: Entry 26 of 26 File: USPT Apr 12, 1994

US-PAT-NO: 5303383
DOCUMENT-IDENTIFIER: US 5303383 A

TITLE: Multiprocessor computer system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Term	Documents
(11 AND 12).USPT.	26
(L11 AND L12).USPT.	26

Display Format: TI Change Format

Previous Page Next Page Go to Doc#

h e b b g e e e f e g ef b e